Minimum Necessary Standard

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

The staff of our organization routinely uses protected health information about patients to carry out their duties. Our staff may also need to disclose protected health information about patients to persons outside the organization or to request protected health information from these persons. Our staff must limit their uses, disclosures, and requests of protected health information to the minimum amount of information necessary to accomplish the purpose of the use or disclosure.

IMPLEMENTATION OF POLICY

This policy does not apply to the following types of uses, disclosures, and requests:

1) Requesting patient information from, or disclosing patient information to, another health care provider for treatment purposes.

2) Disclosing patient information to the patient, or to a personal representative who is authorized to make health care decisions for the patient or the patient's estate.

3) Using or disclosing patient information pursuant to a patient's written authorization.

4) Disclosing protected health information required by the Department of Health and Human Services (HHS) in connection with its investigation or determination of the Organization's compliance with the HIPAA privacy regulations.

5) Using or disclosing protected health information as required by law (not just using or disclosing protected health information in a manner that is permitted by law).

6) Using or disclosing protected health information in order to complete standardized electronic transactions, as required by HIPAA.

ROUTINE USES, DISCLOSURES, AND REQUESTS

The following guidelines explain how much information may be used, disclosed, or requested to carry out routine duties, and who may disclose such information. These guidelines are not intended to restrict organization employees, business associates health care professionals from having access to a patient's entire record, as needed, in order to treat or provide quality care to the patient as determined by the physicians or clinicians applicable.

NON-ROUTINE USES OF PROTECTED HEALTH INFORMATION

Organization staff is instructed to notify the Privacy Official if they believe they need to use protected health information in a way that is not addressed in this policy. The Privacy Official should follow ethical and industry guidelines regarding the use of patient information for treatment and other purposes when making this decision, and should balance the organization's desire to provide quality care and to obtain reimbursement for that care with the patient's interest in privacy. If there is insufficient time to consult with the Privacy Official without jeopardizing patient care, staff member should consider these factors and notify the Privacy Official as soon as possible afterwards.

Many disclosures to persons outside our organization or requests for information from persons outside the organization will require a written authorization from the patient whose protected health information is involved. This policy discusses only how much information may be disclosed or requested and does not discuss when such authorizations are required.

1. Disclosures In Response To Requests From Selected Persons

When the persons or organizations, which have entered into a Business Associates Agreement with our organization are making a request, the Privacy Official or designee may allow the disclosure of the protected health information without second-guessing the request or limiting the amount of information released.

A listing of all Business Associates will be kept by the HIPAA Compliance Officer. They include: billing companies, collection agencies, staffing agencies, cleaning services, copying services, companies ` who provide professional services to the organization.

A health care provider that is required to comply with federal privacy regulations.

A health plan or a health care clearinghouse that converts health information to and from standard and non-standard formats.

A public official or agency requesting protected health information for a public policy purpose.

If the Privacy Official or designee strongly believes that a request by one of the foregoing persons or organizations seeks more than the minimum information necessary, he or she should attempt to reach a compromise that meets the concerns and needs of both the organization and the person or organization making the request.

2. Disclosures In Response To All Other Requests

If the request is made by any other person or organization, the Privacy Official or designee should decide how much information to disclose, using the following criteria:

What is the purpose of the disclosure?

- What type of information does the recipient need to accomplish the purpose of the disclosure?
- Where is this information located? For example, is it in an X-ray? Is it in a medical record? Is it on an electronic database?
- Is other information attached to this information? If so, is the attached information also needed to accomplish the purpose of the disclosure? If the attached information is not needed, a copy of the record should be made and the extraneous information should be redacted (whether electronically or by manually blacking out the information on the hard copy).

3. Requests For Protected Health Information From Others

When deciding what information may be requested from another person or organization outside the Organization, the Privacy Official should consider the following criteria:

What is the purpose of the request? What information is needed to accomplish this purpose?

What other information is likely to be attached to the information the Organization is requesting? If that information is not needed the Privacy Official or designee should specify in the request that this information need not be disclosed.

Can the request be phrased more narrowly to target only the information needed by the Organization to accomplish this purpose?

USING, DISCLOSING, OR REQUESTING THE ENTIRE MEDICAL RECORD

Our staff is instructed to contact the Privacy Official or designee if they believe that the entire medical record should be used, disclosed, or requested in a way that is not addressed as "routine" and is not excepted from this policy, as described above. The Privacy Official or designee will determine whether there is a specific justification for using, disclosing, or requesting the entire medical record. If there is insufficient time to consult with the Privacy Official or designee without jeopardizing patient care, the staff member should consider the factors described above and notify the Privacy Official as soon as possible afterwards. The specific justification for using, disclosing or requesting the entire medical record should always be documented in the patient's medical record.

Organization Privacy/Security Official

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization must have a Privacy/Security Official to oversee and implement the Privacy Program and Security Program and work to ensure the facility's compliance with the requirements of the HIPAA Standards for Privacy & Security of Individually Identifiable Health Information. The Privacy/Security Official is responsible for receiving complaints about matters of patient privacy.

From time to time, our patients may request that we provide certain additional privacy protections for their health information. It is organization policy to respond to all patient requests with careful consideration and respect. Under the law, special procedures must be followed when handling certain types of requests. The following policy addresses the procedures that must be followed by the Privacy/Security Official when handling patient requests for the following types of protections:

Restrictions on uses and disclosures of protected health information
Confidential communications with the patient or patient's personal representative

The Privacy/Security Official, or his or her designee, should carefully review any patient requests for these privacy protections and determine which requirements will apply. Patient requests for privacy protections may only be granted or denied in accordance with the specific requirements below.

IMPLEMENTATION OF POLICY

The Privacy Official must:

establish or identify a committee to be designated with Privacy/Security Program oversight and responsibility;
be a member of the HIPAA Privacy/Security Committee.

Our organization shall designate an appropriate individual to serve as the Privacy/Security Official.

Our organization is responsible for compliance with the requirements of the HIPAA Standards for Privacy & Security of Individually Identifiable Health Information. The Privacy/Security Official responsibilities for implementation and oversight of the Privacy/Security Program include but are not limited to:

1) Privacy Policies and Standards

Communication and implementation of the Privacy Program to the staff.
Assistance with deployment to and implementation by the appropriate policies and procedures related to privacy and security.
Development, communication and implementation of policies and procedures related to patient privacy and security.

2) Training

Overseeing initial and ongoing training for all members of the staff on the policies and procedures related to protected health information as necessary and appropriate to carry out their job-related duties and that training is promptly provided if there are any changes to the policies or procedures.
Ensuring all new members of the staff are trained within a reasonable period of time, preferably during Orientation Training.
Document that training has been provided.

3) Advise members of the staff on privacy/security matters as appropriate.

4) Complaints

Serve as the individual to receive complaints concerning privacy/security rights.
In conjunction with other appropriate parties (*e.g.*, HHS) investigate the complaint.
Document complaints received and their disposition.

5) Sanctions

In conjunction with the appropriate manager, ensure violations of privacy/security policies and procedures are addressed as appropriate pursuant to the human resource policies and procedures.
Document sanctions that are applied.

6) Mitigate, to the extent practicable, any harmful effect that is known from the use or disclosure of protected health information in violation of policies and procedures.

Privacy/Security Program responsibilities include but are not limited to:

1) Compliance with all policies and procedures related to the Privacy Program.
2) Implementation of policies and procedures for patient privacy/security designed to comply with the HIPAA Standards for Privacy & Security of Individually Identifiable Health Information.
3) Creation of and revisions to the policies and procedures promptly as necessary to comply with changes in the law. Changes must be documented and implemented.
4) Provision of a Notice of Privacy Organizations to patients.
5) Compliance with the standards of any Joint Notice and the policies of an organized healthcare arrangement with respect to joint activities.
6) Ensure appropriate administrative, technical, and physical safeguards to protect health information from any intentional or unintentional use or disclosure that is in violation of privacy policies or standards.
7) Ensure any documentation required by the privacy policies be kept for a minimum of 6 years from the effective date.

Patient Access to Protected Health Information

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Patients and their legal representatives generally have a right to access their own health information contained in records that may be used to make decisions about them. It is our policy to treat all patient requests to access such information in a respectful manner. Our organization has strict policies and procedures, however, about how and when patients and their legal representatives may access records. Therefore, patients and their legal representatives should be directed to submit any requests for access to medical records or any other records (whether or not they contain patient health information) to a manager. Only authorized employees may respond to such requests.

IMPLEMENTATION OF POLICY

1. Right To Access Records

What Information. Our patients and their personal and legal representatives (referred to collectively throughout this policy as patients/representatives) have the right to inspect and obtain a copy of the protected health information that our organization, or one of its business associates, maintains in "designated record sets." "Designated record sets" are sets of records that may be used to make decisions about the patients or their treatments.

The designated record set for each patient generally includes the patient's medical records and billing records. The specific records included in a designated record set are discussed in Policy Uses and Disclosures of PHI for Research on preparing and maintaining designated record sets, which specifies what categories and types of records are part of the designated record set.
Patients/representatives also have the right to access protected health information.

For How Long. Patients/representatives have the right to access their protected health information for as long as the information is contained in their designated record sets.
Exceptions. In some circumstances, we may/must deny a patient/representative the right to access protected health information in a designated record set.

In Writing. Requests for access must be made in writing. The manager should encourage the patient/representative to complete the request form Request for Protected Health Information or to write a letter that covers the same information requested on that form.

Follow Up Questions. The manager should follow up on a patient's request if necessary to clarify what information the person is seeking to access. The manager or other authorized personnel should record on the request form the results of that discussion and initial or sign his or her notes.

2. Response Time

Responses to requests for access to protected health information under this policy (by either granting or denying the request) must occur within fifteen (15) days after the request is received.

3. Granting Patient Requests For Access

A patient's/representative's request for access to the patient's protected health information may only be granted according to the following procedures. The manager must complete these procedures within the time provided in Section 2 of this policy, unless the patient/representative chooses to delay access until a later time for his or her own convenience.

Notify the Patient/Representative. The manager must notify the patient/representative that his or her request for access is being granted. The patient/representative may be notified in person, by phone, or in writing. If the patient/representative requested a copy of the records, every effort should be made to provide a copy to the patient/representative when providing the notice informing the patient/representative that the request has been granted or promptly thereafter. If the patient/representative requested an opportunity to inspect the patient's records,

the manager or other authorized personnel must explain how the patient/representative may arrange an appointment to visit the site and review the information.

Requests for Inspection of Records. If permission is granted for a request to inspect protected health information, the manager or other authorized personnel must arrange an appropriate time for the individual to review the records. Copies cannot be provided in lieu of inspection unless (1) the patient/representative agrees, or (2) a ground for denial in Section 4 or Section 5 of this policy justifies providing copies instead of inspection.

• **Proper Identification.** The individual must present proper identification before being permitted to inspect the information. If the person requesting to inspect the information claims to be a personal or legal representative of the patient, proof of the person's relationship to the patient and authority to access records as a personal or legal representative must be presented. The manager or other authorized personnel must be familiar with the policy that explains who may serve as a personal representative of a patient.

• **Supervising Inspection of Records**. The manager of the specific site, or his or her designee, should be present in the room at all times to ensure that the integrity of the records is maintained. The employee should remain in view of the patient/representative to prevent inappropriate tampering, but far enough so that the patient/representative is afforded appropriate privacy when reviewing the content of the records. The employee should not answer any questions regarding the content of the medical record. If the patient/representative wishes to be completely alone, he or she must request copies of the records.

• **Other Issues.** A patient's/representative's review of information should take place only where the patient/representative will not be able to view information or records concerning other patients. A patient may be accompanied by a family member or other individual and may view their records with that companion.

Requests for Copies. Copies of records will be provided in hard copy. Copies should be delivered to the patient/representative in the method specified on the patient's/representative's request form or letter. The patient/representative may visit the site to pick up the copies or request that the copies be delivered by mail to an address provided on the form or letter.

Requests for Digital Copies. Copies of records will be provided primarily on CD unless the individual requests another digital format. Thumb drives will only be accepted if they are in original packaging and there is no evidence of tampering. Our office will keep new, unopened thumb drives which the individual can purchase, at cost. This cost is in addition to the digital copy fee of $10.00. Copies should be delivered to the patient/representative in the method specified on the patient's/representative's request form or letter.

Providing Summaries or Explanations. If the patient's/representative's request to access information is granted, the manager or other authorized personnel may also provide additional items. The following items should be provided if the patient/representative requests the items or agrees to our request to provide the items:

- A summary of the requested information instead of, or in addition to, providing access to inspect or copy the information.
- An explanation of the protected health information contained in the requested records. This explanation would be delivered to the patient/representative when he or she inspects the records, or would accompany the copies of records that are provided to the patient/representative.

Duplicate Information. If the same protected health information is maintained in more than one designated record set, the manager or other authorized personnel need only produce the protected health information once in response to the patient's request. Access need not be provided to records that merely duplicate identical information. However, if a second record provides additional information in any form, that record must be provided.

EXAMPLE: If a patient's physician makes notations on a laboratory report containing the patient's test results, the resulting record will not be considered a duplicate of the original and must also be produced.

Collection of Fees. Our organization charges for copies, preparation of summaries and explanations, and expedited requests. Procedures for the collection of fees vary depending on the items or services provided. If a third party vendor is handling the copying of records, then this policy is not applicable for the vendor.

Charging for medical records copies. In the State of Florida under Chapter 458, F.S. the cost of reproducing copies of written or typed documents or reports shall not be more than $1.00 per page for the first 25 pages and 25 cents for copies over 25. For reproducing x-rays and other special kinds of reports the costs are limited to actual costs that can include material and supplies, labor and overhead cost associated with the duplication. We will not withhold medical records even if you have not received payment for services or the patient has an outstanding balance. As a medical provider we can take up to 30 days to provide access to or copies of an individual's medical records. Our office shall not charge any other fee for paper records. Fees for digital copies of PHI are $10.00.

• **Summaries and Explanations.** Before preparing or providing summaries or explanations, the manager of the specific site should prepare an estimate of the costs of preparing such items. The patient/representative must be notified of the estimated costs of preparing the explanation or summary and given an opportunity to decide whether to continue with the request, modify the request to reduce the costs, or withdraw the request. Ordinarily, the patient/representative must agree to reimburse any estimated costs before any preparation of the requested materials.

□ A fee of $25.00 will be charged to prepare a summary of the information.
□ A fee of $25.00 will be charged to prepare an explanation of the information.

• **Fees.** A receipt must be given to patient and a record of the access provided should be maintained in the patient's chart.

4. **Denying Access Without Opportunity for Review**

Reasons for Denial. In certain circumstances, a patient's/representative's request to access health information should be denied, and the patient/representative will not have any right to challenge or appeal the denial. Those circumstances are:

Notice of Denial. If the request is being denied without an opportunity for review, the manager of the specific site must notify the patient/representative, within the time frame applicable in Section 2 of this policy, using the denial notice. The following procedures should be followed when completing these notices:

Partial Denial. If there are grounds to deny the request as to only part of the protected health information requested, the manager of the specific site is expected to do their best to provide the patient/representative with access to the rest of the information after excluding the parts that cannot be inspected or copied.

- The request is not in writing; or
- The information requested is not contained in a designated record set maintained by our organization or any of its business associates.
- When preparing the denial notice, the manager or other authorized personnel should indicate the grounds for denying the request by checking off the appropriate box or boxes.
- If the request is denied because the our organization does not maintain the information in a designated record set, the manager or other authorized personnel must state in the denial notice any credible information that the manager may have about where the patient/representative may obtain access to the requested records (e.g. inform the patient/representative to submit a request to the hospital where the our organization physician or clinician services were provided.)
- If the request is only partially denied, the manager or other authorized personnel must explain in the denial notice what information the patient/representative will not be permitted to access and what information the patient will be permitted to access.

□ If the patient/representative has requested an opportunity to inspect records, the notice should include instructions about how the person may arrange to examine the records to which access is granted.

□ If the patient/representative has requested copies of the records, the manager or other authorized personnel billing office should include, along with the partial denial notice, copies of those records to which access is granted (after removing the information which the patient/representative is not permitted to access).

5. **Denying Access with Opportunity For Review**

Reasons for Denial. A request to access health information may also be denied if a licensed health care professional (such as a physician, physician's assistant, or nurse) has made certain determinations based upon his or her professional judgment. In these circumstances, the patient/representative will have an opportunity to challenge or appeal the decision by requesting a review. The determinations include:

- A licensed health care professional at our organization has determined that granting the patient's request is reasonably likely to endanger the life or physical safety of the patient or another person. The danger must be to life or physical safety. The request cannot be denied simply because the information is sensitive or has the potential to cause emotional or psychological harm to the patient or another person.
- The information requested refers to another person, and a licensed health care professional at our organization has determined that granting the patient access to this information is reasonably likely to endanger the life or safety of that other person. However, access may not be denied if the person who may be harmed is a health care provider.

EXAMPLE: A physician or mental health clinician at our organization has incorporated information about several patients in his group therapy notes. One of the patients requests access to these notes. The patient's request may be denied if the physician believes that releasing the information contained in those notes is reasonably likely to endanger the life or safety of one or more of the other patients referred to in the notes.

A patient's personal representative is seeking access to the patient's protected health information, and a licensed health care professional at our organization has determined that granting the request is reasonably likely to be injurious to the health or welfare of the patient or could reasonably be expected to endanger the life or safety of any other person.

Partial Denial. If there are grounds to deny the request as to only part of the protected health information requested, the manager of the specific site is expected to do their best to provide the patient/representative with access to the rest of the information after excluding the parts that cannot be inspected or copied.

Notice of Denial. If the request is being denied with an opportunity for review, the manager or other authorized personnel must notify the patient/representative, within the time frame applicable in Section 2 of this policy, using our approved denial notice.

- When preparing the denial notice, the manager or other authorized personnel should indicate the grounds for denying the request by checking off the appropriate box or boxes.
- If the request is only partially denied, the manager or other authorized personnel must modify the denial notice to explain what information the patient/representative will not be permitted to access and what information the patient/representative will be permitted to access.

□ If the patient/representative has requested copies of the records, the manager or other authorized personnel should include, along with the partial denial notice, copies of those records to which access is granted (after removing the information which the patient/representative is not permitted to access).
□ If the patient/representative has requested an opportunity to inspect records, the notice should include instructions about how the person may schedule an appointment to examine the records to which access is granted.

Review Process. If access is denied for any of the reasons provided in Section 5 of this policy, the patient/representative has a right to have the decision reviewed by a licensed health care professional who was not directly involved in the initial decision to deny the request.

- If a patient/representative requests this review, the manager of the specific site must refer the request to the Privacy Official who in turn will refer this on to the Medical Director of our organization.
- The Medical Director of our organization must determine, within a reasonable period of time, whether access was properly denied under any of the grounds provided in Section 5 of this policy, and report his/her results to the Privacy Official who in turn will notify the manager of the specific site responsible for handling the request. In most cases, we would expect a response should be provided within ten (10) days.
- The manager or other authorized personnel must then notify the patient/representative of the results of the review.

Check off the appropriate box indicating the results of the review process.
□ The letter must explain how the patient may file a complaint with our organization or the Department of Health and Human Services.

• If access is required after the review process is completed, the manager of the specific site must follow the procedures in Section 3 of this policy.

6.Documentation

The manager or other authorized personnel must keep the following documentation in connection with any request by a patient/representative to access protected health information. These documents must be maintained by the our organization for six (6) years from the date of their creation:

• The request for access;
• Copies of any notices advising that a fee may be charged to recover the costs of providing copies, summaries, or explanations of the information requested;
• Information about any access provided to the patient/representative;
• A copy of any notice of denial sent to the patient/representative;
• A copy of any notice of review results sent to the patient/representative.

Patient Request to Amend Protected Health Information

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Patients generally have a right to request that our organization amend health information contained in records that may be used to make decisions about the patient. Our organization treats all patients' requests in a respectful manner. Our organization has strict policies and procedures about how and when patient requests for amendment of records will be granted or denied. Therefore, for records maintained by our organization site, patients should be directed to submit requests for amendment of medical records to the Office Manager or other authorized personnel. The request should be processed in a timely and respectful manner in accordance with the procedures below.

IMPLEMENTATION OF POLICY

1. Right To Request Amendment

What Information. Patients have the right to request that we amend the protected health information that our organization, or one of our business associates maintains in "designated record sets." "Designated record sets" are sets of records that may be used to make decisions about the patients or their treatment and generally include the patient's medical record and billing records.

For How Long. Patients have the right to request amendment of their protected health information for as long as the information is contained in the designated record set.

In Writing. All requests for amendment must be made in writing. The Office Manager or other authorized personnel should encourage the patient or the patient's personal representative to complete the request form Request for Correction/Amendment of PHI or to write a letter that covers the same information requested on that form.

Follow Up Questions. Although a patient's request should be made in writing, the Office Manager or other authorized personnel as appropriate should follow up on a patient's request by phone to clarify what information the patient is seeking to amend. The Office Manager or other authorized personnel should record on the patient's request form the results of that discussion and initial his or her notes.

2. Response Time

The Office Manager or other authorized personnel is expected to respond to patient requests for amendment of their protected health information (by either granting or denying the request) as soon as possible after the request is received. At the very latest, the response to the request should be issued within 30 days from the date the request was received. If the patient's written request is not made on the form Request of Correction/Amendment of PHI, the Office Manager or other authorized personnel should write in the equivalent information on whatever written request was submitted by the patient.

3. Granting Requested Amendments

A patient's request for amendment of protected health information may only be granted according to the following procedures. The Office Manager or other authorized personnel must complete these procedures within the time provided in Section 2 of this policy.

Review of Information. The Office Manager or other authorized personnel should determine whether the information that the patient would like to amend was created by our organization. The Office Manager or other authorized personnel should also determine whether the patient would be prohibited from inspecting his or her own information. Our organization cannot amend information that was not created by them unless they have reason to believe that the person or organization that did create the information is no longer available to respond to a request for amendment. Our organization also cannot amend information if the patient requesting the amendment would not be able to inspect the information. The Office Manager or other authorized personnel should review the information to determine if an amendment is appropriate. Where necessary, the manger should consult with the medical staff who created the information or with other staff who might be able to verify information. The Office

The Office Manager or other authorized personnel should only grant a patient's request to amend certain protected health information if they determine that the current information is incomplete or inaccurate and should be amended (completely or in part) as requested by the patient.

Notify the Patient and Obtain Permission To Notify Others. The Office Manager or other authorized personnel must notify the patient may be notified in person, by phone, or in writing.

When providing notice, the Office Manager or other authorized personnel should also ask the patient the following questions:

Would the patient grant our organization permission to notify other persons or organizations that have relied, or may rely, on the original information in a way that may negatively affect the patient?

Would the patient like our organization to notify any other persons about the amendment?

Make the Amendment. The Office Manager or other authorized personnel should make the appropriate amendment everywhere that the patient's protected health information appears in designated record sets maintained by our organization or its business associates. The procedures for correcting the information contained in records should be followed. For example:

If a document is entirely misplaced and does not belong in the patient's record, it may be removed from the record and re-filed in its proper place.

If a document belongs in the patient's record but contains an error, the Office Manager or other authorized personnel should attempt to make a notation directly on the record that corrects the information without deleting the original entry.

If additional pages are required to correct the information, the Office Manager or other authorized personnel should make a notation on the original document directing the reader to the amendment page or pages. Where possible, the amendment page or pages should be physically attached to the original document (for example, using staples).

If the information that needs to be amended is contained in an electronic format, the Office Manager or other authorized personnel should attempt to make a notation that corrects the information without deleting the original entry, or create a link to a location where the amended information can be found.

Notify Others. The Office Manager or other authorized personnel is expected to use all reasonable efforts to forward the amendment to persons or organizations that the patient has stated should be notified. If the patient agrees, this manager is also expected to notify any person or organization that may have relied, or may rely in the future, on the original information in a way that may negatively affect the patient. The patient's agreement is not necessary to notify our organization or business associates.

Future Disclosures. Any future disclosures of the protected health information that needed to be amended must include the amended information or a link to the amended information. If the information needs to be disclosed through a standard transaction that does not permit inclusion of the additional material required by the amendment, the Office Manager or other authorized personnel may separately transmit the amendment material.

4. Denying Requested Amendments

Reasons For Denial. A patient's requested amendment may be denied under the following circumstances:

The request is not in writing;
The patient's request did not explain why he or she believes our organization should make the amendment;
The information is not contained in a designated record set maintained by our organization or any of its business associates;

The information was not created by our organization, unless it has reason to believe that the person or organization that did create the information is no longer available to fulfill the patient's request (for example, if the facility that created the information has closed); and/or
The Office Manager or other authorized personnel cannot determine that the information is inaccurate or incomplete without the requested amendment.

Notice of Denial. If the patient's request for an amendment is denied, the Office Manager or other authorized personnel must notify the patient (within the time frame applicable in Section 2 of this policy) using the approved denial notice.

When preparing the denial notice, the Office Manager or other authorized personnel should indicate the grounds for denying the patient's amendment by checking off the appropriate box or boxes.

If the ground(s) for denying the amendment is that the patient would not be permitted to inspect the information, the denial notice must explain the reason that inspection is not permitted.

If the amendment is only partially denied, the denial notice must explain what portion of the amendment will be granted and what portion will be denied. It must also explain how the patient may contact the our organization if he or she wishes the organization to make the partial amendment.

The partial amendment may not be made without the patient's permission. If the patient grants permission, the Office Manager or other authorized personnel must make the partial amendment in accordance with the procedures in Section 3 of this policy.

The notice must also explain the patient's right to request that we include a statement about the amendment when disclosing the disputed information to other persons in the future.

Statement of Disagreement. After receiving our organization's denial notice, the patient may submit a statement explaining his or her disagreement with our decision. This statement should be limited to 3 pages.

If the patient submits a statement of disagreement, the Office Manager or other authorized personnel may prepare a rebuttal statement if necessary to clarify our organization's position about why the amendment should be denied, or to respond to issues raised in the patient's statement of disagreement. A copy of this rebuttal statement must be provided to the patient. Consultation with the Privacy Official must take place prior to sending the rebuttal to the patient.

Recordkeeping. The Office Manager or other authorized personnel must physically attach, or electronically link, the following documents to the protected health information that was the subject of the disputed amendment (in every place that information appears in the patient's designated record sets):

the patient's written amendment request; Our organization's notice denying that amendment request; the patient's statement of disagreement (if any); and Our organization's rebuttal statement (if any).

Future Disclosures. The following documents must be included in any future disclosures of the patient's information. If the patient's protected health information needs to be disclosed through a standard transaction that does not permit inclusion of the materials required below, the Office Manager or other authorized personnel may separately transmit these materials.

Statement of Disagreement. If the patient has submitted a statement of disagreement, the Office Manager or other authorized personnel must include the following documents, or an accurate summary of these documents, in any future disclosure of the protected health information that is the subject of the dispute.

No Statement of Disagreement. If the patient does not submit a statement of disagreement, he or she may request that our organization includes the patient's amendment request and the denial notice in any future disclosure of the protected health information that is the subject of the dispute. If the patient makes this request, the Office Manager or other authorized personnel must include these documents, or an accurate summary of them, in any future disclosures of the information. If the patient does not make this request (and does not submit a statement of disagreement), the Office Manager or other authorized personnel need not include any of these materials in future disclosures of the protected health information that was the subject of the disputed amendment.

5. Compliance With Amendments Reported From Other Organizations

If another organization informs our organization that it has granted a patient's request to amend the patient's protected health information (and how that information has been amended) the Office Manager or other authorized personnel must amend that patient's protected health information *everywhere* it appears in designated record sets maintained by our hospital. These amendments should be made in accordance with the procedures set forth in Section 3 of this policy, including notifying the patient and others (where appropriate) that the amendment has been made.

6. Forwarding Response to the Privacy Official

After responding to each amendment and/or Denial of Protected Health Information, a copy of this data must be forwarded to the Privacy Official.

Authorization for Release of Protected Health Information and Revoke Authorization

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization must obtain a written authorization from a patient prior to using or disclosing of protected health information (PHI) for the purposes described in the implementation section of this policy and in our Notice of Privacy Organizations (the "Notice").

IMPLEMENTATION OF POLICY

Authorization for uses and disclosures of protected health information (PHI) must be obtained for:

1) Uses and disclosures outside of treatment, payment, and health care operations, unless otherwise allowed;
2) Uses and disclosures created for research;
3) Psychotherapy notes except:
    a) To carry out treatment, payment, or health care operations:
    Use by the originator of the notes for treatment;
    Use or disclosure in training programs in which trainees, students, or practitioner in mental health learn under supervision to organization or improve their skills in group, joint, family, or individual counseling; or Use or disclosure by a facility to defend a legal action or other proceeding brought on by the individual.
    b) Use and disclosure with respect to oversight of the originator of the notes.

"Psychotherapy notes" means: notes recorded (in any medium) by a physician or clinician who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items; diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

The provision of treatment to an individual may not be conditioned on signing an authorization except for:
1) Research-related treatment; and
2) Health care that is solely for the purpose of creating information for disclosure to a third party.
An individual may revoke an authorization in writing except to the extent that:
1) The facility has taken action in reliance thereon; or
2) If an authorization was obtained as a condition of obtaining insurance coverage.

PROCEDURE:

1) In general, all written authorization must be obtained using the authorization forms in this policy. However, any signed form presented by a patient or his/her representative that contains the required information is acceptable.
2) Every signed authorization must be documented and retained for a minimum of six (6) years.
3) An authorization for use of PHI may not be combined with any other document to create a compound authorization, except as follows:

An authorization for the use and disclosure of PHI created for research may be combined with any other type of written permission for the same research study, including another authorization or a research informed consent.

An authorization for use or disclosure of psychotherapy notes may only be combined with authorization for use or disclosure of psychotherapy notes.

An authorization in accordance with this policy, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other authorization except when the provision of treatment or payment has been conditioned on the provision of one of the authorizations.

Uses and Disclosures of PHI for Research De-Identification Process Creation of Limited Data Set

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Protected Health Information obtained by our organization may not be used internally or disclosed to any persons or organizations outside our organization for research purposes without ensuring that strict policies and procedures regarding access, use, and disclosure of protected health information for research purposes are followed.

IMPLEMETATION OF POLICY

Certain requirements apply to the use and disclosure of protected health information in connection with research involving human subjects. As a rule, the organization may not authorize the use or disclosure of protected health information for research purposes except:

For reviews preparatory to research;
For research on the protected health information of a decedent;
If our organization has obtained the informed consent of the individual to participate in the research, or a waiver of such informed consent, prior to April 14, 2003 (this exception ceases to apply if informed consent is sought from the individual after April 14, 2003);
If the information is completely "de-identified";
If the information is partially de-identified into a "limited data set" and the recipient of the information signs a data use agreement to protect the privacy of such information;
If our organization has obtained a valid authorization from the individual subject of the information.

The specific requirements for each of these exceptions are discussed below.
Special rules apply to the use and/or disclosure for research purposes of psychotherapy notes.
The management of the organization must determine that one of the exceptions described below applies for permitting the use and disclosure of any protected health information for research purposes. Management of the organization should require either an individual authorization or must grant a waiver of authorization if none of the other exceptions apply. All research activities must also comply with other applicable policies relating to research and with any additional requirements that apply to the specific types of information identified above as having special rules.
Finally, to the extent that our employees provide treatment to subjects as part of a research study, they must follow other policies to the extent those policies apply to the provision of health care to individuals.

1. Research Defined

For purposes of this policy, research includes any systematic investigation (including research development, testing, and evaluation) that has as its primary purpose the development of or contribution to generalizable knowledge.

Generalizable knowledge. Knowledge may be generalizable even if a research study only uses protected health information held within the organization and the results are generalizable only to the population served by the organization. Research is therefore not limited to clinical trials funded by government sponsors (such as the National Institutes of Health) or commercial sponsors. Quality assurance and utilization management activities do not typically result in generalizable knowledge and thus ordinarily would not be governed by this policy.

Primary purpose. The development or contribution to generalizable knowledge must be the primary purpose of the investigation for this policy to be applicable. In some instances, the primary purpose of the activity may change as preliminary results are analyzed. An activity that was initiated as an internal hospital outcome evaluation, for example, may produce information that administration intends to generalize. If the purpose of a study changes and the results will be generalized, the investigator must document the change in status of the activity and obtain approval from organization management.

Research authorization. The subjects' permission to use and disclose PHI.

If an activity would be considered "research" under other applicable policies, it should be considered research for purposes of this policy. However, research that is exempt under the Common Rule may not be exempt under HIPAA and the procedures set forth in this policy must be followed with respect to such research.

2. General Prohibition and Exceptions

Organization management may not authorize the use or disclosure of protected health information for research purposes unless at least one of the following exceptions applies:

Reviews Preparatory to Research. Organization management may permit the use and disclosure of protected health information to develop a research protocol or for similar purposes preparatory to research (*e.g.*, to determine whether the organization has information about prospective research participants that would meet the eligibility criteria for enrollment in a research study). The preparatory research provision of the HIPAA Privacy Rule 45CFR 164.512(i)(1)(i) et seq. permits covered entities to use or disclose PHI as an aid to study recruitment, although it does not permit the researcher to remove PHI from the covered entity's site. The provision allows a researcher to identify prospective research participants for purposes of seeking authorization to use or disclose PHI for a research study.

A researcher who is not part of the covered entity may not use the preparatory research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of authorization by organization management. Actual contact would have to be made by someone who works as part of the covered entity and reasonably has access to the protected health information.

In order to permit the use or disclosure of protected health information under this exception, organization management must obtain representations from the researcher that:

- The use or disclosure is sought solely to prepare a research protocol or for similar purposes preparatory to research;
- No researcher will remove any protected health information from the organization's premises in the course of the review; and
- The protected health information for which use or access is sought is necessary for the research purposes.

During the preparatory review, those granted access may only record information in a form that is "de-identified."

Research on the Protected Health Information of a Decedent. Organization management may permit the use and disclosure of the protected health information of a decedent for research purposes. In order to permit such a use or disclosure, organization management must:

- Obtain representations from the principal investigator that the use or disclosure is sought solely for research on the protected health information of a decedent (*e.g.*, researchers may not request a decedent's medical history to obtain health information about a decedent's living relative); and/or
- Verify that the information for which use or disclosure is sought is necessary for the research purposes.

Informed Consents or Waivers of Informed Consent Obtained Prior to April 14, 2003.

Organization management may approve the use or disclosure of protected health information for a specific research project provided that one of the three following requirements are met:

Express Legal Permission for Use and Disclosure of Protected Health Information. If the researcher has obtained, prior to April 14, 2003, express legal permission from the individual that *specifically authorizes* a use or disclosure of protected health information for purposes of the research project, organization managementmay permit such use or disclosure for purposes of that project. However, any restrictions on the use and disclosure of health information provided in such express legal permission must be honored.

General Informed Consent. If the researcher has obtained, prior to April 14, 2003, the individual's informed consent to participate in a specific research project, organization management may permit the use or disclosure for purposes of that project even though the informed consent does not specifically authorize the use or disclosure of protected health information for purposes of the research project. However, any restrictions on the use and disclosure of health information provided in such informed consent must be honored.

Waiver of Informed Consent. If the researcher has obtained, prior to April 14, 2003, an I.R.B. waiver of the informed consent requirement (in accordance with the Common Rule) for a specific research project, organization management may permit a use or disclosure of the individual's protected health information for purposes of that project. However, if the researcher obtains an individual subject's informed consent at any time after April 14, 2003,

the researcher will also be required to obtain the individual's Research Authorization (as provided in this policy) at that time.

Completely De-identified Information. Organization management may allow completely de-identified information to be used and disclosed for research purposes without restriction. Information may only be considered completely de-identified when either (1) a qualified statistician documents his or her determination that the risk of identification is very small, or (2) the information meets the requirements described in Appendix A of this policy. If organization management has any doubts as to whether protected health information has been completely de-identified within the meaning of this policy, the information should be treated as though it were not completely de-identified and neither used nor disclosed for research purposes without meeting another exception.

Limited Data Set. Organization management may allow the use and disclosure for research purposes of a limited data set including a partially de-identified subset of the individual's protected health information, provided that the person using or receiving the information has signed a Data Use Agreement through which he or she agrees to protect the privacy of the information received. Appendix B of this policy provides more information about the identifiers that must be removed from an individual's protected health information in order to create a limited data set.

Subject Authorization for Research. Organization management may allow the use and disclosure of protected health information pursuant to a completed and signed Research Authorization. Permissible uses and disclosures are limited to those described in the authorization, even though those permissible uses and disclosures may be more limited than what our organization's Notice of Privacy Organizations describes.

The Research Authorization must be completed by the principal investigator for the research subject's review and signature. It is the responsibility of the principal investigator to ensure that the Research Authorization covers the uses and disclosures necessary for the research study.

When obtaining a Research Authorization, an individual's ability to receive research-related treatment as part of a research study may be conditioned upon the individual's agreement to sign the Research Authorization form. However, in presenting the Research Authorization form to prospective subjects, researchers should never suggest that failure to sign the form will limit access to any treatment that may be available outside the study.

Approval of Waiver. Organization management may allow the use and disclosure of protected health information for research purposes if organization management grants a partial or total waiver of the authorization requirement. If organization management grants only a partial waiver – that is, if it modifies or waives only some elements of the Research Authorization form – organization management must condition the use and/or disclosure of any protected health information for research purposes on compliance with any authorization requirements not waived and as modified. For example, if organization management grants a partial waiver of authorization to allow a researcher to obtain protected health information to recruit potential research participants, the researcher would still have to obtain Research Authorizations from the subjects to use and disclose protected health information to conduct the research study.

3. Individual Access

Individuals generally have a right to access all their protected health information maintained by our organization or its business associates. Any patient requesting access to protected health information obtained in the course of research (including protected health information that may be contained in research records) should be directed to submit his or her request to the office manager via the Form: Patient Access to Protected Health Information, which provides detailed guidelines for responding to such requests. The manager of the specific site will determine, with assistance from the researcher and the Privacy Official, whether access to protected health information should be denied under any of the exceptions described in that policy.

4. Documentation

Organization management must retain any writings or documentation required by this policy for six years from the date of its creation or the date when it last was in effect, whichever is later.

Appendix A

COMPLETE DE-IDENTIFICATION

Information is completely de-identified if none of the following 18 types of identifiers is contained in the information and if no one accessing the information has actual knowledge that the information could be used – alone or in combination with other information – to identify any individual who is the subject of the information. Note that this does not prohibit coding records so that they may later be re-identified, so long as the code does not contain information about the subject of the information (for example, the code may not be a derivative of the individual's Social Security Number) and is not used or disclosed for any other purpose, and so long as the re-linking mechanism (e.g., the subject log or coding algorithm) is not disclosed to any persons or organizations outside our organization.

1. Names
2. All geographic subdivisions smaller than a State, including:
   street
   address
   city
   county
   precinct
   zip codes, except for the initial three digits of a zip code if, according to the current publicly-available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. Telephone numbers
4. Fax numbers
5. E-mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. All elements of dates (except year) for dates related to an individual, including:

    birth date
    admission date
    discharge date
    date of death
    all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying numbers, characteristics, or codes

Appendix B

CREATION OF LIMITED DATA SET

Organization Management may approve the use and disclosure of a limited data set for research purposes if the person who would use or receive the information has signed a Data Use Agreement through which the person agrees to protect the privacy of the information received.

A limited data set may be created by removing from the individual's protected health information the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. Postal address information, other than town or city, state, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

Note: Limited data sets may also be used and disclosed for the organization's or the recipient's health care operations and for public health purposes, but requirements for the use and disclosure of a limited data set for these non- research purposes are set forth in the data use agreement. Any questions concerning use and disclosure of a limited data set for research or non-research purposes should be directed to Privacy/Security Official or his or her designee.

Requests for Restrictions on Use or Disclosure of PHI

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Individuals have a right to request restrictions on uses and disclosures of PHI about the individual to carry out treatment, payment and health care operations, and disclosures made to family members or persons who are involved in the health care of the individual. Health care components are not required to agree to such requested restrictions unless the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment) and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.
All restrictions to which the health care component agrees must be documented and retained.

IMPLEMENTATION OF POLICY

A. Agreeing to a Restriction

If our organization agrees to a requested restriction, PHI must not be used or disclosed in violation of the agreed upon restriction, except that the information may be used by the health care component or disclosed to another health care provider when the information is necessary for emergency treatment of the individual. If the health care component discloses PHI to a health care provider for emergency treatment purposes, the health care component must request that the information not be further used or disclosed by the provider.
Agreed upon restrictions are not effective to limit uses or disclosures as permitted or required to the Secretary for compliance, for a facility directory or for disclosures made for a public purpose.

B. Terminating an Agreed Upon Restriction

Agreed upon restrictions may be terminated if the individual agrees to or requests termination in writing or orally. Our organization will document all oral requests. Our organization may terminate an agreed upon restriction without the individual's agreement to the termination by informing the individual. However, such terminations by our organization are effective only as to PHI created or received after the individual is given notice of the termination.

C. A Restriction Not To Disclose Information to An Insurance Company

Per the Final Rule implements the requirement of Section 13405(a) of the HITECH Act with respect to allowing individuals to request restriction of disclosures of PHI relating to services for which out-of-pocket payment was made by the individual. Upon an individual's request, our organization must now agree to restrict disclosure of PHI about the individual to the health plan if (1) the disclosure is for the purpose of carrying out payment or healthcare operations and is not otherwise required by law; and (2) the PHI pertains solely to a healthcare item or service for which the individual, or person other than the health plan on behalf of the individual, has paid our organization in full.
The following procedures will be followed:

a. Our organization requires that the individual sign “Do Not File Insurance Waiver” for each incident where the individual restricts disclosures of PHI to their insurance company.
b. The Office Manager/HIPAA Compliance Officer will log all such requests and keep them for a period of six (6) years.
c. The Office Manager/HIPAA Compliance Officer is responsible for ensuring that the requested disclosure is not permitted to be disclosed as a part of the insurance company’s chart or other reviews of the organization’s records and documentation.
d. The individual’s right to Restriction Not to Disclose Information to an Insurance Company shall be posted on our Notice of Privacy Organizations.

Requests for Confidential Communications

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization must permit the individual to request, and must accommodate reasonable requests to receive communications of PHI from the health care component by alternative means or locations.
This request by the individual must be in writing and may be conditioned on provision of information on how payments will be handled and specification of an alternative address or method of contact.
The provider components may not require an explanation from the individual of the reason for requesting the confidential communication. If deemed necessary, our organization may require assertion of danger to the individual as a condition to providing the confidential communication.

IMPLEMENTATION OF POLICY

A. **Making the Request for Confidential Communications**

. The following procedures will be followed:

a. Our organization requires that the individual fill out the form "Request for Confidential Communications" .
b. This information is to be entered into the patient's file with a note/flag stating this is the only proper method of communication with the individual.
c. It is the responsibility of the Office Manager/HIPAA Compliance to determine if the request by the individual is "reasonable".
d. All documentation is to keep kept for a period of six (6) years.

Patient Privacy - Accounting of Disclosures

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization patients have a right to an "accounting of disclosures," which includes information about many disclosures of the patient's protected health information that the organization has made to third parties. It is the group organization policy to treat all patient requests in a respectful manner. If a patient asks questions about obtaining an accounting of disclosures for services provided by our organization the patient should be directed to make his or her request to the Office Manager or the Privacy Official.

IMPLEMENTATION OF POLICY

Because a patient may request an accounting at any time, the manager of the specific area must record, on an ongoing basis, all information that could possibly be needed to respond to a patient's future request. Any manager of the specific area who discloses a patient's protected health information MUST complete a Disclosure Form, unless an exception applies below. Completed Disclosure Forms should be added to the patient's medical record, billing records, or Privacy Official record as applicable.

Each and every member of our staff will be expected to comply with this policy of recording disclosures. Seemingly minor violations (such as skipping information required on forms) may be subject to disciplinary action because such violations may make it impossible for the group organization to supply accurate information to patients requesting an accounting of disclosures.

1. Types of Disclosures Which Need Not Be Recorded

Our organization is required to keep records of certain disclosures of a patient's protected health information and to provide an accounting of those disclosures to patients who request such an accounting. Disclosure means a release, transfer, or provision of access to or divulging in any other way of information outside our organization. This means that disclosures to persons who are not part of our organization must be accounted for unless an exception applies. **The staff should note that the following activities are not considered "disclosures" and therefore need not be recorded:**

Sharing protected health information for treatment purposes;

Sharing patient information with any other covered entity that is part of an organized health care arrangement for treatment, payment and health care operations pertaining to the activities of the applicable organized Health Care Arrangement;

Certain disclosures to other covered entities for payment and operations of that covered entity with respect to patients of the covered entity;

Disclosures made pursuant to the patient's specific written authorization;

Disclosures to the patient or the patient's personal representative;

Disclosures made to the patient's friends and family (in accordance with the Our organization Notice of Privacy Organization Policy or a Joint Notice provided on behalf of an organized health care arrangement);

Disclosures that are incidental to an otherwise permitted use or disclosure (and thus unavoidable despite taking all reasonable precautions to avoid the disclosure);

EXAMPLE: During the course of a treatment session, other patients in the treatment area may see, or overhear discussion of, a patient's health information despite the Our organization staff's efforts to take all precautions to speak softly.

Disclosures made for national security and intelligence purposes;

Disclosures made about inmates to correctional institutions or law enforcement officials; and

Disclosures made before April 14, 2003.

2. Information Required For Each Disclosure

The following information must be included for each disclosure on the Disclosure Form:

The date of the disclosure;

The name of the person or organization that received the information;

The address of the person or organization that received the information (if known);

A brief description of the protected health information disclosed (with dates of treatment when possible); and

• At least one of the following items:

A brief statement explaining the purpose of the disclosure and the basis on which the disclosure was permitted under our policies, *or*

A copy of a written request made by a person or organization to whom disclosure was made where the information was disclosed for one of the public policy reasons permitted.

3. Provision of the accounting:

1. The facility must act on the individual's request for an accounting, no later than 30 days after receipt of such a request, as follows:
   a. The facility must provide the individual with the accounting requested; or
   b. If the facility is unable to provide the accounting within the time required then the facility may extend the time to provide the accounting by no more than 30 days, provided that:
      i. The facility, within the time limit set provides the individual with a written statement of the reasons for the delay and the date by which the facility will provide the accounting; and

      ii. The facility may have only one such extension of time for action on a request for an accounting.

1. The facility must provide the first accounting in any 12-month period to an individual. The facility may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the facility informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

4. Documentation

A facility must document the following and retain the documentation for six years:

1. The information required to be included in an accounting;
2. The written accounting that is provided to the individual which should be stored with the permanent record; and
3. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

5. EXCEPTION:

Series of Disclosures: If a series of disclosures were made to the same person or organization on the basis of a single written authorization form, staff need only include the information above for the *first* disclosure made during the accounting period. Staff may then provide the following information to cover the rest of the series:

. Frequency, periodicity, or number of disclosures made in the series, and

. EXAMPLE: Disclosures were made every 2 months.

EXAMPLE: A total of 15 disclosures were made during the accounting period.

The date of the last disclosure in the series that was made during the accounting period.

Disclosure for Certain Research Activities -Waiver of Authorization

If our organization has made disclosures of PHI for a particular research purpose in accordance with HIPAA Privacy Standards § 164.512 (i) for 50 or more individuals, the accounting may provide:

1. The name of the protocol or other research activity;
2. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
3. A brief description of the type of PHI that was disclosed;
4. The date or period of time during which such disclosure occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
5. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
6. A statement that the PHI of the individual may or may not have been disclosed for a particular research protocol or other research activity.

If our organization provides an accounting for research disclosures in accordance with the Research section noted above and at the request of the individual, the covered entity must assist in contacting the entity that sponsored the research and the researcher if it is reasonably likely that the PHI of the individual was disclosed for research protocol or activity.

Examples of Disclosures That Need To Be Tracked

1. Reports of child abuse, neglect, or domestic violence.
2. Any disclosure required by law (state encounter data, infectious disease reporting, etc.).
3. Disclosures to funeral directors, coroners, and medical examiner.
4. Disclosures in accordance with a judicial subpoena.
5. Public health activities (births, deaths, public health investigations, adverse events, work related injuries, FDA required reporting, etc.
6. Health oversight activities (audits and investigations by Government benefit or regulatory programs).
7. Specialized government functions (law enforcement custodial situations).
8. Disclosure for certain law enforcement purposes (identification of a suspect or missing person, identification of a crime victim, suspected crime, etc.).
9. Disclosures to organ procurement and banking organizations.
10. Disclosures to a third party when the safety of an individual is at risk (threat of violent Workers' compensation disclosures.
11. Disclosures made in error (e.g. faxed to a wrong number or message left on the wrong answering machine).

Confidentiality of Protected Health Information

SCOPE OF POLICY

This policy applies to all members of our organization, its participating business associates, and all organization employees and business units who provide management, administrative, financial, legal, and operational support to or on behalf of our organization.

STATEMENT OF POLICY

Our organization is committed to protecting the privacy and confidentiality of health information about its patients. Protected health information is strictly confidential and should never be given, nor confirmed to anyone who is not authorized to receive this information.

IMPLEMENTATION OF POLICY

A. Definition of Protected Health Information

For purposes of the policy, the term "protected health information" means any patient information, including very basic information such as their name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

This policy applies to protected health information in any form including spoken, written, or electronic form. It is the responsibility of our organization to protect the privacy and preserve the confidentiality of all protected health information. This includes, but is not limited to, compliance with the protective procedures below.

B. Public Viewing/Hearing

The staff of our organization is expected to keep protected health information out of public viewing and hearing. For example, protected health information should not be left in conference rooms, out on desks, or on counters or other areas where the information may be accessible to the public or to other employees or individuals who do not have a need to know the protected health information. Medical staff and support staff should also refrain from discussing protected health information in public areas, such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more patients. Medical staff and support staff should also take care in sharing protected health information with families and friends of patients. Such information may generally only be shared with a personal representative, a family member, relative, or close personal friend who is involved with the patient's care or payment for that care. Even in the latter circumstance, information cannot be disclosed unless the patient has had an opportunity to agree or object to the disclosure, and staff may only disclose information that is relevant to the involvement of that family member, relative, or close personal friend in the patient's care or payment for the patient's care, as the case may be.

C. Databases and Workstations

The staff of our organization is expected to ensure that they exit any confidential database upon leaving their workstations so that protected health information is not left on a computer screen where it may be viewed by individuals who are not authorized to see the information. They are also expected not to disclose or release to other persons any item or process which is used to verify their authority to access or amend protected health information, including but not limited to, any password, personal identification number, token or access card, or electronic signature. Each employee is responsible for all activity occurring under his or her account, password, and/or electronic signature. These activities may be monitored.

D. Downloading, Copying, or Removing

The staff should not download, copy, or remove from the clinical areas any protected health information except as necessary to perform their duties. Upon termination of employment with our organization, or upon termination of authorization to access protected health information, the employees must return to the organization any and all copies of protected health information in their possession or under their control.

E. Emailing and Faxing Information

The staff of our organization should not transmit protected health information over the Internet (including e-mail) and other unsecured networks unless it has been encrypted and password protected, and the Security Officer approves the process used. Transmission of protected health information is permitted by fax using the following guidelines:

1. Always include a cover sheet with the faxed information and confidentiality statement:

   The documents accompanying this transmission contain confidential privileged information. The information is the property of the sender and intended only for use by the individual or entity named above. The recipient of this information is prohibited from disclosing the contents of the information to another party.

   If you are neither the intended recipient or the employee or agent responsible for delivery to the intended recipient, you are hereby notified that disclosure of contents in any manner is strictly prohibited. **Please notify [name of sender] at [facility name] by calling [phone #] immediately if you received this information in error.**

2. Limit manual faxing to urgent transmittals:

   A. Faxing PHI is appropriate only when the information is needed immediately for patient care.

   B. Medical emergencies (*e.g.* ER or emergency surgery).

   C. Other situations considered urgent (*e.g.* results from lab to physicians).

3. Unless necessary to treat in emergency situations, highly sensitive or personal information should be strictly limited when faxing. In general, this information should not be faxed:

   A. Drug dependency

   B. Alcohol dependency

   C. Mental illness or Psychiatric information

   D. Sexually transmitted disease (STD) information

   E. HIV status

   F. Genetic test results

4. There are times when faxing highly sensitive information would be appropriate:

   Example: Faxing PHI to a hospital's emergency room regarding the HIV status of a pregnant patient in labor.

5. Location of the Fax Machine:

   A. Should be secure whenever possible.

   B. Make sure that area is not accessible to the public.

   C. When possible, locate the machine in an area that requires security keys or badges for entry.

6. Mitigation of faxes sent to the incorrect party or sent in error:

   A. Organization should make reasonable efforts to obtain the copies from the recipient and see that they are destroyed.

   B. If copies cannot be retrieved due to number of copies and cost to return, and the fax recipient is a known business associate, verbal documentation of the destruction of the information is sufficient.

   C. If the information is inadvertently sent to a patient-restricted party or to a recipient where there is a risk of release of the PHI (*e.g.* newspaper), the Privacy Official should be notified and legal counsel should become involved for further instructions.

Privacy Complaint Process

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Under the Privacy Standards, a patient may file a complaint with the facility, as well as with the Secretary of the U.S. Department of Health and Human Services. The purpose of these complaint mechanisms is to instill a measure of accountability. The organization has a complaint process in place that will be utilized to handle privacy complaints.

IMPLEMENTATION OF POLICY

1. The person or office that handles the privacy complaints is: Privacy/Security Official or his or her designee.
2. The information gathered should include the following: (See HIPAA Kit Patient Complaint Form)
    - Name of the Complainant
    - Date the complaint was filed
    - Date and time of the incident (if applicable)
    - Location
    - Names if any members of the workforce who were involved
    - Name of physician or clinician that was involved
    - Short summary of the dispute

3. Receipt of a complaint must be acknowledged in writing by the Privacy/Security Official or designee.

4. The Privacy/Security Official or designee will develop and maintain an investigation/disposition report that identifies any privacy deficiencies discovered in the investigation and the steps taken. The Privacy/Security Official or designee will send a report regarding the disposition of the investigation to the complainant and a copy will be maintained by the Privacy/Security Official or designee.

Should a complaint against a workforce member or physician be found to be valid, the disposition of such complaint will be consistent with the facility's Sanctions for Privacy Violations.

Privacy/Security Training

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

All employees who are employed by our organization are required to complete certain training (the "Training") on HIPAA Privacy and Security. The **Training** must be completed within the first 30 days of employment. There is initial training reading material that is required before any staff member is allowed access to PHI or EPHI. The workforce member after reading this initial security/privacy training must sign an acknowledgement of completion.

IMPLEMENTATION

Training will be provided to all staff.

Requirements are as follows:

1. The Privacy/Security Official is responsible for the development and implementation of, and compliance with, privacy and training. The HIPAA Privacy/Security Committee will act as an advisory group.
2. All members of the staff will be trained on privacy policies and organizations within thirty (30) days of hire date and thereafter, upon any material change.
3. All members of the staff will be trained on privacy policies as part of their applicable orientation process.
   a. New employees must view a HIPAA presentation approved by the Privacy/Security Official and may be required to take a quiz.

   b. Passing grade of 60% or better is required on the quiz. If this is not achieved, then a repeat viewing of the HIPAA presentation with a retake of the quiz is required. If a passing grade of 60% or better is not achieved on the retake, then the Privacy/Security Official will meet with the individual employee.

4. Documentation must be kept for at least six years on all members who have been trained on privacy/security policies and organizations.
5. Security reminders will be disseminated throughout the year to remind employees of security and privacy requirements.
6. All regularly scheduled staff meetings will contain information on HIPAA security.

Policy on Passwords

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

IMPLEMETATION OF POLICY

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of our entire corporate network. As such, all employees (including contractors and vendors with access to systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All passwords that access EPHI must be changed on at least every 90 days.
- All other passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days. Each employee/workforce member must have a unique user I.D.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All passwords must conform to the guidelines described below.

Guidelines

A. General Password Construction Guidelines

Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. All workforce members should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

The password is a common usage word such as:

Names of family, pets, friends, co-workers, fantasy characters, etc.
Computer terms and names, commands, sites, companies, hardware, software.
Our company name,
Birthdays and other personal information such as addresses and phone numbers.
Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
Any of the above spelled backwards.
Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

Contain both upper and lower case characters (e.g., a-z, A-Z)
Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
Are not a word in any language, slang, dialect, jargon, etc.
Are not based on personal information, names of family, etc.
Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for company accounts as for other non-company access (e.g., personal ISP account, option trading, benefits, etc.).
Do not share your passwords with anyone, including administrative assistants or secretaries.
All passwords are to be treated as sensitive, confidential information.

Here is a list of "don'ts":

Don't reveal a password over the phone to ANYONE
Don't reveal a password in an email message
Don't reveal a password to the boss
Don't talk about a password in front of others
Don't hint at the format of a password (e.g., "my family name")
Don't reveal a password on questionnaires or security forms
Don't share a password with family members
Don't reveal a password to co-workers while on vacation
If someone demands a password, refer them to HIPAA Compliance Officer
Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).
Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
Change passwords at least once every 90 days.
If an account or password is suspected to have been compromised, report the incident to HIPAA Compliance Officer and change all passwords.

I agree to abide by this Policy on Passwords:

_____

Employee Signature

Employee Name:

Date:

Requirements During Disasters

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Notification. During times of disaster our organization and its associated clinics will be permitted to disclose Protected Health Information to public or private entities authorized by law or by their charter to assist in disaster relief efforts. Disclosures may be made to assist in the notification of (including identifying or locating) a family member or personal representative of an individual, or another person responsible for the care of the individual, of the individual's location, general condition, or death. Our organization providers should ask for the individual's agreement to such disclosures, or give the individual an opportunity to object, to the extent that doing so would not interfere with the ability to respond to emergency circumstances.

Secretary's Waiver During Emergency. Pursuant to the Project BioShield Act of 2004, the Secretary of the United States Department of Health and Human Services (the "Secretary") is authorized to waive penalties for failing to comply with certain provisions of the HIPAA Privacy Regulations. If the Secretary issues such a waiver, then our organization will, as necessary and consistent with the waiver, suspend compliance with the following HIPAA Privacy Regulations, for the period of time specified by the Privacy/Security Official:

A. The requirement to obtain a patient's permission before speaking to family and/or friends;
B. The requirement to honor a request to opt out of any facility directory;
C. The requirement to distribute a Notice of Privacy Organizations;
D. The requirement to allow a patient to request confidential communications; and
E. The requirement to allow a patient to request privacy restrictions.

After this time our organization will comply with the above HIPAA Privacy Regulations requirements with respect to any patient still under its care. Our organization shall not take any actions pursuant to a waiver in a manner that discriminates among individuals on the basis of their source of payment or their ability to pay.

Verification of Identity. In an emergency our organization will permit the disclosure of Protected Health Information to other providers (e.g., physicians, hospitals) even if the outside providers are not known to our organization, providing the staff member exercises reasonable professional judgment to ensure that the person/entity to whom information is being disclosed is, indeed, a treatment provider. For example, a organization provider may respond to a request from a hospital seeking protected health information in a circumstance described as an emergency, if the organization provider determines that the patient's interests are best served by making the disclosure.

Policy on Marketing Activities

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization may not use or disclose protected health information for marketing without an authorization signed by the patient. No marketing communications may be made without the prior approval of the Privacy/Security Official or designee in accordance with the following procedures.

IMPLEMETATION OF POLICY

1) **Definition of Marketing.** Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

Marketing does not include communications:

a) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of our organization including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits;

b) For treatment of the individual; or

c) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

An arrangement between our organization and any other entity whereby our organization discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service is always marketing, notwithstanding the above.

2) **Authorization for Marketing.** Our organization may not use or disclose protected health information for marketing without an authorization signed by the patient, unless the communication is in the form of:

a) A face-to-face communication made by our organization to an individual; or

b) A promotional gift of nominal value provided by our organization.

Policy on Fundraising Activities

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization may not use or disclose protected health information for fundraising without an authorization that meets the applicable requirements under HIPAA except as defined below. Organization management must authorize all fundraising activities in accordance with this policy.

IMPLEMETATION OF POLICY

This policy is based on principles related to the uses and disclosures of protected health information for fundraising.

1. Our organization may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization:
    a. Demographic information relating to an individual; and
    b. Dates of health care provided to an individual.

2. Our organization must include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving any further fundraising communications.

3. Our organization must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

4. Organization Management shall maintain a list of all patients who have opted out and provide a copy of said list annually to the Privacy/Security Official.

5. The use of Protected Health Information (PHI) for fundraising purposes other than as described herein is prohibited without a patient authorization, which meets the HIPAA.HITECH requirements.

Personal Representatives/Minors

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

This policy addresses (1) personal representatives and (2) the privacy rights of minors under the age of 18 who are not emancipated from the care of their parents or guardians.

Personal representatives are those individuals who, under Florida law, are able to make health care decisions on behalf of the patient. With respect to deceased individuals, a personal representative is an executor, administrator, or other person who has authority to act on behalf of the deceased individual or of the individual's estate. With respect to the protected health information relevant to their personal representation, personal representatives have the same rights and obligations as the patient for all purposes under our organization's HIPAA policies and procedures, except with respect to the *Patient Access to Protected Health Information* policy.
Under Florida's Civil Code, patients under the age of 18 may be emancipated from the care of a parent or guardian by court or if they are married. *Emancipated individuals will be afforded the same privacy rights as all adults in accordance with all other organization HIPAA policies.*

As a general rule, only the parent, guardian or other person acting in the place of a parent (collectively referred to as "parents or guardians" has the authority to control, access and protect the confidentiality of protected health information about a minor. In limited circumstances, however, a minor will have the authority to exercise these rights on his or her own behalf. Clinicians and staff are expected to protect the privacy of health information about minors in accordance with the procedures below.

IMPLEMENTATION OF POLICY

A. General Rule: Control By Parent or Guardian

As with personal representatives generally, parents or guardians ordinarily have the authority to control the health information of a minor by exercising the rights granted to a patient concerning his or her health information. For example, a parent or guardian typically has the authority to do the following:

- Sign an authorization form permitting the use and disclosure of the minor's information for other purposes;
- Object to the use and disclosure of the minor's information in the hospital directory, or to friends and family involved in the minor's health care;
- Inspect or copy the minor's information;
- Request amendment of the minor's information;
- Request an accounting of disclosures of the minor's information;
- Request additional privacy protections, including confidential communications, with respect to a minor's information;
- Request a copy of the hospital's Notice of Privacy Organizations';
- File privacy complaints with the hospital or with the United State Department of Health and Human Services.

Note that there are certain circumstances, such as a medical emergency, under which our organization may provide treatment to a minor without the consent or other written permission of a parent or guardian. In these circumstances, the parent or guardian nevertheless retains the authority to control the privacy of the minor's protected health information. For example, if a ten year old boy is injured in a school bus accident, he may be treated without the consent of a parent or guardian if such consent cannot quickly be obtained. Staff would not, however, be permitted to treat the ten year old boy as having independent authority to exercise his privacy rights. The boy's parent or guardian has the authority to exercise the boy's privacy rights, and staff should obtain a HIPAA Notice of Privacy Organizations from the parent or guardian as soon as practicable after the medical emergency has ended.

B. Exception To General Rule: Minor's Authority to Exercise Privacy Rights

There are two exceptions to the general rule, under which the minor is permitted to exercise the privacy rights listed in Section A of this policy on his or her own behalf:

1. When the minor may lawfully obtain a healthcare service without the consent of a parent, guardian or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service even if a parent or guardian has also consented to the health care service or the minor has voluntarily chosen to involve the parent or guardian in his or her health care. Under Florida law, a minor who is or believes himself or herself to be addicted to a narcotic or other drug may consent to substance abuse treatment, and any minor who believes himself or herself to be afflicted with an illness or disease may likewise consent to care.

Under Florida law, a minor may consent to medical care or the administration of medication for the purpose of alleviating or reducing pain, discomfort, or distress of and during labor and childbirth.

In the above cases, upon the advice and direction of the treating physician, a physician may, but is not obligated to, inform the spouse, parent, or guardian of any such minor as to the treatment given or needed, and such information may be given to, or withheld from the spouse, parent or guardian without the consent and over the express objection of the minor, *unless* an exception in Section C of this policy applies.

2. When a parent, guardian, or other person acting *in loco parentis* agrees to confidentiality between our organization and the minor with respect to a particular health care treatment or service.

C. Abuse, Neglect or Endangerment

A licensed member of our organization as a health care professional may elect not to treat a person as the personal representative of a patient, including a minor, if he or she:

Reasonably believes that the patient (1) has been or may be subjected to violence, abuse or neglect by the person, or (2) could be endangered if the person is treated as a personal representative; and

Decides, using his or her professional judgment, that it is not in the best interest of the patient to treat the person as a personal representative.

Response to Breach of Unsecured PHI

SCOPE OF POLICY

This policy applies to our organization, its participating business associates, and all organization employees.

STATEMENT OF POLICY

Our organization is required by law to protect the privacy of health information that may reveal the identity of a patient. If a breach of certain types of individually identifiable health information occurs, our organization is required to provide notification to certain individuals and entities pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the HITECH Omnibus Rule of 2013 and any regulations promulgated there under (HITECH). Our organization may have additional reporting obligations under other federal laws and state breach notification laws. Those obligations are not addressed in this policy with the exception that Florida laws require notice within 45 days.

IMPLEMENTATION OF POLICY

A. Definition of Breach

For the purposes of the policy, the term "breach" means the acquisition, access, use or disclosure of protected health information in a manner not otherwise permitted under the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. The term "protected health information" means any patient information, including very basic information such as their name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

B. Report of Breaches to Privacy/Security Official

It is the responsibility of our organization to protect and preserve the confidentiality of all protected health information. To avoid possible breaches of protected health information and inform the members of our organization of the importance of promptly reporting privacy and security incidents and the consequences for the failure to do so, the Privacy/Security Official will coordinate with other officials and departments to train all members of our organization on their respective responsibilities and obligations under HIPAA and HITECH, which will include a review of the protective procedures. *See Confidentiality of Protected Health Information*. In addition to training the members of
our organization, the Privacy/Security Official may re-evaluate persons authorized to access protected health information to determine if authorization is necessary and, if necessary, whether such access complies with the minimum necessary standard under HIPAA.

Any member of our organization who knows, believes, or suspects that a breach of protected health information has occurred, must report the breach to the Privacy/Security Official or management immediately. Within one business day of its receipt of a report, the Privacy/Security Official will notify management (or vice versa).

After a potential breach is reported, the Privacy/Security Official will work with management and departments, and the information technology department to conduct a thorough investigation, which includes an analysis to determine whether a breach of unsecured protected health information under HITECH has occurred and if so, what notifications are required. The Privacy/Security Official should complete its investigation generally within [20] calendar days to ensure sufficient time for the preparation and coordination of notifications, if required, provided that the investigation may take more or less time depending on the circumstances. As part of the investigation, the Privacy/Security Official will take all necessary steps to mitigate any known harm. The details of the investigation will be documented in a memo that is kept on file with the Privacy/Security Official with a copy sent to management.

As part of the Privacy Official's investigation to determine whether a breach of unsecured protected health information under HITECH has occurred, the Privacy/Security Official must take certain steps to ensure a complete investigation. The Privacy/Security Official must first decide whether the information is protected health information and if so, whether the protected health information is unsecured.

If the information is not protected health information because, for example, the information is de-identified in compliance with HIPAA, or does not include certain identifiers as set forth in HIPAA, no further investigation is required under HITECH. The Privacy/Security Official will have other responsibilities, including evaluating whether notifications are required pursuant to the Red Flag Rules and/or applicable state breach notification laws.

If the information is protected health information, the Privacy/Security Official will then need to determine if the information has been properly "secured" by the methods set forth in HITECH (e.g. encryption and destruction). If the Privacy/Security Official determines that the protected health information is "secured," although no further steps are required pursuant to this policy, the Privacy/Security Official is responsible for determining whether our organization has accounting and mitigation obligations under HIPAA. If it is determined that the protected health information is unsecured, the Privacy/Security Official must determine whether a breach under HITECH has occurred (see Part C).

The Privacy/Security Official must document the analysis performed to determine if the information is protected health information, and if, necessary, whether the protected health information is secured, in a memo to be kept on file with the Privacy/Security Official with a copy to be sent to management.
As discussed in more detail in Part D below, if a breach under HITECH has occurred and notifications are required, the time period by which notifications must be sent to the affected individuals, the Secretary, and if, necessary, the media begins when the breach is first discovered, not when the Privacy/Security Official completes its investigation of whether a breach has occurred. A breach is treated as discovered when our organization

(i) has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach; or
(ii) is deemed to have knowledge of the breach because a workforce member or agent of our organization has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach.

The Privacy/Security Official will document when the Privacy/Security Official reasonably believes the breach occurred.

C. Determination of Breach

If the Privacy/Security Official has determined that there is an acquisition, access, use or disclosure of unsecured protected health information, the Privacy/Security Official must then conduct the following analysis:

1. Determine whether there has been an impermissible acquisition, access, use, or disclosure of protected health information under the HIPAA Privacy Rule.

2. If no, no further analysis required pursuant to this policy. If yes, determine whether the impermissible acquisition, access, use, or disclosure compromises the security or privacy of the protected health information.

3. If no, no further analysis required pursuant to this policy. If yes, determine whether an exception applies.

1. Impermissible Acquisition, Access, Use, or Disclosure

Protected health information may only be used or disclosed pursuant to a valid authorization or one of the specifically enumerated exceptions under HIPAA. To determine if protected health information was impermissibly acquired, accessed, used or disclosed under the HIPAA Privacy Rule, the Privacy/Security Official will conduct an analysis (the results of which will be detailed in a memo that is kept on file with the Privacy/Security Official with a copy sent to management). If the acquisition, access, use, or disclosure is permitted, no further investigation pursuant to this policy is required. If the Privacy/Security Official determines that an impermissible acquisition, access, use, or disclosure has occurred, he/she is responsible for complying with the applicable policies and procedures (including making an accounting of such disclosure and, if necessary, mitigating any known harm) and conducting the analysis set forth in #2 below.

2. Compromises the Security or Privacy of Protected Health Information

If there has been an impermissible acquisition, access, use, or disclosure of unsecured protected health information under the HIPAA Privacy Rule, the Privacy/Security Official must then perform a risk assessment to determine if there is a significant risk of financial, reputational or other harm to the individual whose protected health information was used or disclosed. The Privacy/Security Official will consider a number of factors, including:

Who impermissibly disclosed or to whom the information was impermissibly disclosed (i.e. was the acquisition, access, use, or disclosure to a covered entity or business associate, or to a private individual or entity). There may less risk of harm to the individual if the recipient of the information is obligated by HIPAA and HITECH.

The likelihood the information is accessible and usable by the unauthorized individual.
Whether our organization has taken immediate steps to mitigate, including obtaining assurances from the recipient that the information will not be further used or disclosed, or that the information is destroyed or returned prior to it being improperly accessed.

The type and amount of protected health information involved. The Privacy/Security Official must examine the information that was acquired, accessed, used or disclosed, including whether the information involved the name of the individual and that services were received, the types of services received or where the services were received (i.e. at a specialized facility or department) and if the information increases the risk of identity theft (i.e. SSN, account number or mother's maiden name). The Privacy/Security Official should carefully conduct a fact intensive investigation that includes any type of health information that may cause reputational harm.

The Privacy/Security Official will document the risk assessment in a memo that is kept on file with the Privacy/Security Official with a copy sent to management. If the Privacy/Security Official determines that there is no significant risk of harm to the individual, no further steps need to be taken pursuant to this policy. The Privacy Official, however, is responsible for conducting a separate analysis regarding our organization's accounting and mitigation obligations, if any.

3. Exceptions to the Definition of Breach

If, based on the above analysis, the Privacy/Security Official determines that there has been an impermissible acquisition, access, use, or disclosure which compromises the security or privacy of the protected health information, the Privacy/Security Official must determine if any of the following exceptions apply:

Any unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;

Any inadvertent disclosure by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received from such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or

Disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

The Privacy/Security Official will perform a fact specific analysis to determine if an exception applies and document its analysis and findings in a memo that is kept on file with the Privacy/Security Official with a copy sent to management. If an exception applies, the Privacy/Security Official can conclude that a breach did not occur and that no notification is required.
If none of these exceptions apply, the Privacy/Security Official must conclude that a breach of unsecured protected health information has occurred and notification to affected individuals, the Secretary of HHS (Secretary) and, if applicable, the media is required.

D. Breach Notification

Once the Privacy/Security Official has determined that a breach has occurred, he/she is responsible for coordination of a response to certain persons and entities.

Notification to Affected Individuals

Notification must be provided to each individual whose unsecured protected health information has been or is reasonably believed to have been, acquired, accessed, used or disclosed as a result of the breach without unreasonable delay and in no case later than 45 calendar days. If the breach requires the involvement of law enforcement, the notification may be delayed for a period of time as determined by a law enforcement official.

The Privacy/Security Official must prepare a notification that includes (to the extent possible):

A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

Any steps individuals should take to protect themselves from potential harm resulting from the breach;

A brief description of what our organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, web site or postal address.

The Privacy/Security Official will be sensitive to only include general information (i.e. listing the types of information involved as opposed to listing the actual protected health information that was involved in the breach) in the notification. Depending upon the nature of the breach and the information obtained during the investigation, the Privacy/Security Official may also include

Recommendations that the individual contact applicable credit card companies and information about how to obtain credit monitoring services;

Information about the steps our organization is taking to retrieve the breached information and improve security to prevent future breaches; and

Information about sanctions our organization imposed on its workforce members involved in the breach.

To comply with other applicable laws, the Privacy/Security Official may also need to translate the notice into other languages and make the notice available in alternate formats, such as Braille, large print or audio.

The Privacy/Security Official will send a draft of the notice to management and, if available a media consultant, for review. The preparation and review of the notice should be completed within [15] calendar days (more or less time may be necessary depending on the circumstances).

The notice will be sent by first-class mail or, if our organization does not have sufficient contact information for some or all of the affected individuals, by substitute notice (depending on the number of individuals for whom our organization does not have sufficient contact information, through an alternate form of written notice, by telephone or other means, or by a posting on the organization web site for 90 days or in major print or broadcast media in geographic areas where the affected individuals likely reside).

Notification to the Secretary

The Privacy/Security Official must provide notice to the Secretary concurrently with the notification sent to the affected individuals (for any breach involving 500 or more individuals) or within 60 days after the end of each calendar year (for breaches involving less than 500 individuals). In the latter case, the Privacy/Security Official will maintain a log and other documentation of each breach to ensure that the scope and extent of the information provided to the Secretary is in compliance with HITECH. The content of the notice will be the same as described above.

No later than November 30 of each year, the Privacy/Security Official and the Information Security Officer will meet to discuss the process and content of the report to be sent to the Secretary. The Privacy/Security Official and Information Security Officer will prepare a draft of the report and by January 31, will send the draft to management. By February 15, management, the Privacy/Security Official and the Information Security Officer will finalize the report for submission to the Secretary on or before March 1.

Notification to the Media

The Privacy/Security Official may also be required to notify a prominent media outlet for any breach that involves more than 500 residents of any one state or jurisdiction. The notification will contain the same information

as described above and will be made concurrently with the notification sent to the affected individuals. The Privacy Official, depending on the circumstances of the breach, will determine what constitutes a prominent media outlet.

The Privacy/Security Official will be responsible for documenting that all notifications required under HITECH were made in a memo to be kept on file with the Privacy/Security Official with a copy to be sent to management.

Notification by Business Associates

Management will work with business associates of our organization to ensure that business associates report any breaches of protected health information promptly to the appropriate individual at our organization.

To the extent the unsecured protected health information is the protected health information of a covered entity that participates in an organized health care arrangement with our organization, thee Privacy/Security Official will coordinate with the respective Privacy Official(s) of such covered entities.

QUESTIONS: If you have questions about this policy, please contact the Privacy/Security Official immediately.